

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

Chambers of
Joseph A. Dickson
United States Magistrate Judge

Martin Luther King, Jr. Federal Bldg.
& U.S. Courthouse
50 Walnut Street
Newark, New Jersey 07102
(973-645-2580)

LETTER OPINION

October 13, 2020

All counsel of record via ECF

Re: Gaaays In Spaaace v. John Does (1-10) et al.
Civil Action No.: 20-12412(BRM) (JAD)

Counsel:

This will address Plaintiff Gaaays In Spaaace's ("GIS") unopposed motion for leave to serve a third-party subpoena prior to the Rule 26(f) conference in this matter. (ECF No. 3). Pursuant to Federal Rule of Civil Procedure 78, the Court resolves Plaintiff's application without oral argument. Upon careful consideration of the submissions, and for the reasons stated below, Plaintiff's motion is **GRANTED**, subject to certain restrictions set forth herein.

I. BACKGROUND

This action involves Defendants alleged unauthorized access and misuse of computer and email systems owned and operated by the Plaintiff.

On September 8, 2020, Plaintiff filed a Complaint against "John Doe" defendants identified only by a single IP address, asserting claims for violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 and the Stored Communications Act, 18 U.S.C. § 2701 (See generally Compl. (ECF No. 1)). Plaintiff alleges that Defendants conspired to illegally hack into the computer and email systems operated by Plaintiff. (Pl.'s Br. in Support of Mot. ("Pl.'s Br.") at ¶ 3 (ECF No. 3)). On May 2, 2020 multiple attempts to access the GIS systems allegedly proved fruitful and the

intruders successfully changed the passwords of the email accounts used by GIS Team Members—rendering them inoperative to GIS for its business purposes. (*Id.* at ¶¶ 3–5 (ECF No. 3)).

According to Plaintiff, review of system logs produced an IP address in New Jersey that accessed multiple GIS accounts. (*Id.* at ¶ 8 (ECF No. 3)). This review determined that the following IP address accessed a GIS Account: 73.231.8.205. (*Id.* at ¶ 12 (ECF No. 3)). This same IP address, according to the plaintiff, is one issued by Comcast Cable. (*Id.* at ¶ 8 (ECF No. 3)). Plaintiff, in an effort to identify this individual, now moves to serve Comcast Cable Communications, LLC with a subpoena seeking identifying information on the customer assigned that IP address under the Cable Communications Policy Act of 1984, 47 U.S.C. § 551. (*Id.* at ¶¶ 15–26 (ECF No. 3)).

II. LEGAL STANDARD AND ANALYSIS

Fed. R. Civ. P. 26(d)(1) provides that “[a] party may not seek discovery from any source before the parties have conferred as required by Rule 26(f).” The Court, however, may grant leave to conduct discovery prior to that conference. *Id.* In ruling on a motion for expedited discovery, the Court should consider “the entirety of the record to date and the reasonableness of the request in light of all of the surrounding circumstances.” Better Packages, Inc. v. Zheng, No. 05-4477, 2006 WL 1373055, at *2 (D.N.J. May 17, 2006) (quoting Merrill Lynch, Pierce, Fenner & Smith, Inc. v. O’Connor, 194 F.R.D. 618, 624 (N.D. Ill. 2000)). Courts faced with motions for leave to serve expedited discovery requests to ascertain the identity of John Doe defendants in internet copyright infringement cases, for instance, often apply a “good cause” test. See In re Bittorrent Adult Film Copyright Infringement Cases, No. 11-3995(DRH), 2012 WL 1570765 (E.D.N.Y. May 1, 2012) (granting limited early discovery regarding a John Doe defendant); Pacific Century Int’l. Ltd. v. Does 1-101, No. 11-2533, 2011 WL 5117424, *2 (N.D. Cal. Oct. 27, 2011) (finding plaintiff had not shown good cause to obtain expedited discovery).

Good cause exists where “the need for expedited discovery, in consideration of the administration of justice, outweighs the prejudice to the responding party.” Am. Legalnet, Inc. v. Davis, 673 F. Supp. 2d 1063, 1066 (C.D. Cal. 2009); accord Semitool, Inc. v. Tokyo Electron Am., Inc., 208 F.R.D. 273, 275 (N.D. Cal. 2002). This Court has routinely applied the “good cause” standard to permit limited, early discovery under nearly identical circumstances. See, e.g., Malibu Media, LLC. v. John Does 1-11, No. 12-7615 (CCC), 2013 U.S. Dist LEXIS 26217 (D.N.J. Feb. 26, 2013). In that case, the plaintiff sought leave to serve a subpoena demanding that the ISP in question reveal the John Doe defendants’ names, addresses, telephone numbers, e-mail addresses and Media Access Control addresses. Id. at *3-4. This Court granted the plaintiff’s request for early discovery, but only permitted the plaintiff to obtain the information absolutely necessary to allow it to continue prosecuting its claims: the defendant’s name and address. Id. at * 3. The Court imposed that limitation due to concerns that the person whose information was on file with the ISP might not be the same person who engaged in the allegedly infringing activity (i.e., others, including persons outside of the household, may have been responsible), and because more expansive discovery could impose an undue burden on such innocent individuals. Id. at *9-11 (citing Third Degree Films, Inc. v. John Does 1-110, Civ. A. No. 2:12-cv-5817, 2013 U.S. Dist. LEXIS 27273 (D.N.J. Jan. 17, 2013)).

Other courts in this District have reached the same conclusion and have imposed similar limitations. See, e.g., Malibu Media, LLC v. Doe, No. 13-4660 (JAP) (DEA), slip op. (ECF No. 5) at 2 (D.N.J. Aug. 19, 2013) (limiting the scope of a pre-Rule 26(f) conference subpoena to a subscriber’s name and address); Voltage Pictures v. Doe, No. 12-6885 (RMB) (JS), 2013 U.S. Dist. LEXIS 155356, *9-10 (D.N.J. May 31, 2013) (granting leave to serve subpoena requesting only the name, address and media control address associated with a particular IP address); Malibu

Media, LLC v. John Does 1-18, No. 12-7643 (NLH) (AMD), 2013 U.S. Dist. LEXIS 155911, *9-10 (D.N.J. Mar. 22, 2013) (restricting the scope of a pre-Rule 26(f) conference subpoena by not permitting discovery of the internet subscriber's telephone number or e-mail addresses).

Here, the Court finds good cause to permit limited discovery prior to the Rule 26(f) conference. Without information from Comcast, Plaintiff will likely be unable to amend its Complaint to name the appropriate defendant, let alone effectuate service of that pleading. See Patrick Collins, Inc. v. Does, No. 12-3907 (ES)(CLW), 2012 WL 12903893 at *2 (D.N.J. Aug. 17, 2012) (finding good cause shown where Plaintiff essentially holds no other way to obtain the true identity of a subscriber other than using the IP address as a means to obtain the information from the Internet Service Provider). In essence, Plaintiff would be unable to litigate the alleged violations at issue in this matter in any meaningful way. Cf. Id. at *2 (stating that “unless and until the Defendants are identified, this matter cannot proceed forward, and it is likely that Plaintiff will suffer ongoing harm. Moreover, there is a risk an ISP will destroy its logs prior to the conference.”)

Moreover, while the Court recognizes that the subscriber whose information is on file with the ISP may not be personally responsible for the allegedly wrongful access; he or she may have information that assists in identifying the infringer. The subscriber's identity is therefore relevant and discoverable under the broad scope of Rule 26. See Malibu Media, LLC v. Does, No. 12-07789 (KM) (MCA) 2013 U.S. Dist. LEXIS 183958, *24 (D.N.J. Dec. 18, 2013) (“The Court notes that it is possible that the Internet subscriber did not download the infringing material. It is also possible, however, that the subscriber either knows, or has additional information which could lead to the identification of the alleged infringer. Accordingly, the Court finds that the information sought by the subpoena is relevant.”).

While the Court finds that some early discovery is necessary to assist Plaintiff in identifying the individuals allegedly accessed its systems, the Court remains cognizant of the impact that the disclosure of the information Plaintiff seeks might have on an innocent subscriber. Malibu Media, 2013 U.S. Dist. LEXIS 26217 at *10. Even if the Court permits Plaintiff to obtain the expedited discovery it requests, that information would not necessarily reveal the appropriate defendant's identity. It will, rather, only provide information regarding the ISP subscriber. Plaintiff would then have to determine whether that subscriber illegally accessed and compromised the systems. See Pac. Century Int'l Ltd. v. Does, C-11-02533 DMR, 2011 WL 5117424 (N.D. Cal. Oct. 27, 2011). In other words, Plaintiff will likely have to go beyond the limited discovery noted above to confirm the proper Defendant's identity. Id. The burdens associated with the potentially expansive and intrusive discovery that Plaintiff may need to propound in order to definitively identify the correct defendant would likely outweigh Plaintiff's need for expedited discovery. Id. (citations omitted). The Court must therefore endeavor to fashion a remedy that will adequately protect all parties' rights. See In re BitTorrent Adult Film Copyright Infringement Cases, 2012 WL 1570765, *1, *13.

As a result, then, the Court grants Plaintiff's motion, subject to certain limitations. Plaintiff may serve Comcast with a subpoena pursuant to Federal Rule of Civil Procedure 45. That subpoena, however, may only seek the name and address of the subscriber (IP address 73.231.8.205) who allegedly accessed the computer systems and email accounts as outlined in Plaintiff's Complaint. Additionally, Plaintiff shall attach a copy of this Letter Opinion to the subpoena. Information obtained from the ISP shall only be used for the purposes of this litigation,

and Plaintiff shall be prepared to provide copies of the responsive information to any defendant who enters an appearance in this case.¹ The Court will enter an appropriate form of order.

/s/ Joseph A. Dickson
JOSEPH A. DICKSON, U.S.M.J.

Dated: October 13, 2020

cc: Hon. Brian R. Martinotti, U.S.D.J.

¹ If Plaintiff seeks leave to file an amended pleading naming a specific defendant, it shall ensure that it has a factual basis for asserting that the proposed defendant engaged in the alleged misfeasance. By permitting this discovery, the Court is not finding that Plaintiff may rely solely on the subscriber's affiliation with the IP address in question as the basis for its claims.